Paul R. Kiesel, State Bar No. 119854
kiesel@kiesel.law
Jeffrey A. Koncius, State Bar No. 189803
koncius@kiesel.law
Nicole Ramirez, State Bar No. 279017
ramirez@kiesel.law
KIESEL LAW LLP
8648 Wilshire Boulevard
Beverly Hills, CA 90211-2910
Tel: 310-854-4444
Fax: 310-854-0812

Jason 'Jay' Barnes (admitted *pro hac vice*)
jaybarnes@simmonsfirm.com
Eric Johnson (admitted *pro hac vice*)
ejohnson@simmonsfirm.com
An Truong (admitted *pro hac vice*)
atruong@simmonsfirm.com
SIMMONS HANLY CONROY LLC
112 Madison Avenue, 7th Floor
New York, NY 10016
Tel.: 212-784-6400
Fax: 212-213-5949

Michael W. Sobol, State Bar No. 194857
msobol@lchb.com
Melissa Gardner, State Bar No. 289096
mgardner@lchb.com
Jallé H. Dafa, State Bar No. 290637
jdafa@lchb.com
LIEFF CABRASER HEIMANN & BERNSTEIN, LLP
275 Battery Street, 29th Floor
San Francisco, CA 94111-3339
Tel: 415-956-1000
Fax: 415-956-1008

Douglas Cuthbertson (to be admitted *pro hac vice*)
dcuthbertson@lchb.com
LIEFF CABRASER HEIMANN & BERNSTEIN, LLP
250 Hudson Street, 8th Floor
New York, NY 10013
Tel: 212-355-9500
Fax: 212-355-9592

Counsel for Plaintiffs and the Proposed Classes

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE DIVISION

JOHN DOE I , et al., on behalf of themselves and all others similarly situated,
Plaintiffs,

v.

GOOGLE LLC,

Defendant.

Case No. 5:23-cv-02431-BLF

CLASS ACTION

PLAINTIFFS' NOTICE OF MOTION AND MOTION FOR PRELIMINARY INJUNCTION AND PROVISIONAL CLASS CERTIFICATION

Judge: Hon. Beth Labson Freeman
Date: November 2, 2023
Time: 9:00 a.m.
Ctrm.: 3

TO ALL PARTIES AND THEIR COUNSEL OF RECORD:

PLEASE TAKE NOTICE that on November 2, 2023, at 9:00 a.m., or as soon thereafter as this matter may be heard before the Honorable Beth Labson Freeman, in Courtroom 3 of the United States District Court for the Northern District of California, San Jose Courthouse, 280 South 1st Street, San Jose, CA 95113, Plaintiffs John Doe I and John Doe II (together, "Plaintiffs") will and hereby do move the Court pursuant to Rule 65 of the Federal Rules of Civil Procedure for a preliminary injunction ordering Defendant Google, LLC ("Defendant" or "Google") to comply with its statutory and common law obligations by doing the following:

1. Prohibit Google from continuing to acquire Health Information from Health Care Providers through Tracking Technologies associated with Google's advertising systems and products, including Google Analytics, Google Ads, Google Display Ads, Google Tag Manager, Google APIs and YouTube ("Google Source Code"). As used herein, the following terms have the meanings described below:

a. "Health Information" means information protected by the Health Insurance Portability and Accountability Act ("HIPAA") or the California Confidentiality of Medical Information Act ("CMIA") under 45 C.F.R. § 160.103 and Cal. Civ. Code § 56, respectively, and includes information that reveals or tends to indicate patient status; patient portal activity (including but not limited to log-in and log-out activity); appointment information; healthcare payment or insurance information; and communications about doctors, conditions, treatments, medications, symptoms, diagnoses or prognoses regardless of whether those communications occur inside an "authenticated" patient portal or on a property designed for patients that does not require patients to login. The Court's definition is modeled after the HHS Bulletin regarding the "Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates."

b. "Health Care Providers" includes all health care providers, covered entities, and business associates whose information is protected by HIPAA or the

CMIA. *See* 45 C.F.R. § 160.103; Cal. Civ. Code § 56. This includes doctors, clinics, psychologists, dentists, chiropractors, nursing homes, pharmacies, health insurance companies, pharmaceutical companies, and business associates such as vendors Cerner and Epic that operate online patient portals. *See id.*[1]

c. "Tracking Technologies" means "a script or code on a website or mobile app used to gather information about users as they interact with the website or mobile app." The Court's definition is modeled after the HHS Bulletin regarding the "Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates."

Specifically, Plaintiffs ask that Google be prohibited from continuing to acquire such information as follows:

a. First, Google shall, within 14 days of this Order, cease acquiring Health Information from the Health Care Provider web properties identified in the Declaration of Richard Smith at ¶¶ 61 *et seq.* These include: Kaiser Permanente (https://healthy.kaiserpermanente.org); MedStar Health (https://www.medstarhealth.org); Mercy Medical Center (Baltimore, MD) (https://mdmercy.com/); Gundersen Health System (https://www.gundersenhealth.org/); Mercy Hospital (https://www.mercy.net); United Healthcare (https://www.uhc.com); and, OSF HealthCare (https://www.osfhealthcare.org/).

b. Second, Google shall review and respond to the list of Health Care Provider web-properties identified through the expert analysis described in the Declaration of Tim Libert at ¶¶ 14-23, and provided by Plaintiffs to Google. For any web property for which Google agrees that it is acquiring Health

[1] As detailed below, Plaintiffs have identified 6,046 web-properties from which Google tracks and collects Health Information from Health Care Providers; and are providing the list to Google.

Information relating to Health Care Providers through Tracking Technologies on these properties, then Google shall: (i) provide a list of those web properties to Plaintiffs' counsel within 14 days of this Order (ii) cease acquiring such information with 14 days of providing that list to Plaintiffs' counsel.

c. Third, Google shall use its internal tools, including its "verticals" classification system to identify other Health Care Provider web-properties (outside of the list of the Health Care Providers provided by Plaintiffs to Google) from which Google is acquiring Health Information and Google shall: (i) provide a list of those web properties to Plaintiffs' counsel within 14 days of this Order; and (ii) cease acquiring such information within 14 days of providing that list to Plaintiffs' counsel.

d. Fourth, Google shall provide the Court with an update on the status of its compliance with this order 30, 60, 90, and 120 days after the Order issues.

2. Prohibit Google from using patients' Health Information that it has collected from Health Care Providers through its use of Google Source Code. Specifically, for each of the steps above, Google shall be required to remove Health Information from its advertising systems no later than 30 days after it ceases acquiring Health Information from any specific Health Care Provider property.

3. Order Google to take all reasonable steps to immediately preserve, maintain, sequester, segregate, and impound all data, documents, and information, including electronically stored information, that may be potentially relevant to this Action, and to confirm in writing that it has done so along with the specific steps it has taken, including to identify the types or categories of data being preserved. Such preservation shall occur on systems outside of Google's advertising architecture such that the information is not used for advertising purposes, consistent with the Court's order that Google case using Health Information.

4. Provisionally certify the following class pursuant to Federal Rules of Civil Procedure 23(b)(2) for purposes of entering preliminary injunctive relief:

> All persons in the United States whose Health Information was obtained by Google from their Health Care Provider.

5. Appoint John Doe I, John Doe II, Jane Doe I, Jane Doe II, Jane Doe III, Jane Doe IV and Jane Doe V as representatives of the Class and appoint Plaintiffs' counsel, Simmons Hanly Conroy LLC, Kiesel Law LLP, and Lieff Cabraser Heimann & Bernstein, LLP, as interim class counsel.

6. Order such other and further relief that the Court deems just and appropriate.[2]

* * *

Plaintiffs move for preliminary injunction on the basis that Google uses the Google Source Code to track, intercept and collect Plaintiffs' unique identifiers, along with content of communications that they exchange with their Health Care Provider (which include communications exchanged on authenticated and unauthenticated webpages). Google then monetizes that information through its advertising systems for financial gain. Google's conduct is unlawful and ongoing, and the acquisition and use of Plaintiffs' Health Information caused and continues to cause irreparable harm. Moreover, the impact of Google's conduct on the Class – indeed the public at large – is far-reaching. Plaintiffs' evidence demonstrates that, in an analysis of 6,046 Health Care Provider web properties, the Google Source Code is present on **87%** of the Health Care Provider web properties. Impact on the public is not just a probability; it is almost a guarantee. As demonstrated below, Plaintiffs and the putative class they represent (hereinafter, the "Class") will suffer irreparable harm if Google is allowed to continue tracking, collecting, and intercepting patients' communications. Moreover, the balance of equities strongly favors Plaintiffs and the Class, and the requested injunctive relief serves the public interest because the innocent and unnamed parties in this action – namely, the Class – have been deprived of their right to privacy in their

[2] In a similar case pending in front of Judge Chhabria (*DOE v. Google LLC*, Case No. 4:23-cv-02343), the plaintiffs ask the court there to order Google to immediately delete the data at issue. Plaintiffs here do not seek such relief and are concerned that granting such request would result in the destruction of relevant evidence needed for Plaintiffs to hold Google accountable for its misconduct. As a result, Plaintiffs here believe that the data at issue should be preserved for the pendency of the litigation, and only deleted later pursuant to consultation with Plaintiffs' counsel and their consulting experts at that time, subject to court approval.

medical information and communications and Google's conduct will continue to affect patients of medical providers around the country without this Court's intervention.

Plaintiffs further move for provisional class certification on the grounds that the Class is sufficiently numerous, there are ample common questions of law and fact, Plaintiffs' claims are typical of those of the Class, Plaintiffs are adequate representatives, and certification under Rule 23(b)(2) is appropriate because Plaintiffs at this stage seek only preliminary injunctive relief based on Google's practices that are applicable to all Class Members. *See* Fed. R. Civ. P. 23(a), 23(b)(2); *Meyer v. Portfolio Recovery Assocs., LLC*, 707 F.3d 1036, 1041-43 (9th Cir. 2012); *Rodriguez v. Hayes*, 591 F.3d 1105, 1125-26 (9th Cir. 2010).

Plaintiffs also move for appointment of their counsel, Simmons Hanly Conroy LLC, Kiesel Law LLP, and Lieff Cabraser Heimann & Bernstein, LLP, as provisional class counsel under Rule 23(g). The firms have performed substantial work identifying and investigating potential claims, have significant experience prosecuting class actions and other complex cases with claims similar to those at issue here, are knowledgeable regarding the applicable law, and have the resources and ability to litigate this case. *See* Fed. R. Civ. P. 23(g)(1).

Plaintiffs' Motion is based on this Notice of Motion, the accompanying Memorandum of Points and Authorities, the Declaration of Jay Barnes (with seven plaintiff and class member declarations attached), the Declaration of expert Richard Smith, the Declaration of expert Tim Libert, the Declaration of expert Zubair Shafiq, Proposed Order, the pleadings and records on file with the Court, and any further briefing and arguments of counsel.

Respectfully submitted,

Dated: June 13, 2023

SIMMONS HANLY CONROY LLC

By: */s/ Jay Barnes*
Jay Barnes

Dated: June 13, 2023

KIESEL LAW LLP

By: */s/ Jeffrey A. Koncius*
Jeffrey A. Koncius

Dated: June 13, 2023

LIEFF CABRASER HEIMANN
& BERNSTEIN, LLP

By: */s/ Michael W. Sobol*
Michael W. Sobol

Attorneys for Plaintiffs and the Proposed Class

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes and Codes

Other Authorities

Rules

I. STATEMENT OF ISSUES TO BE DECIDED

Plaintiffs respectfully request that the Court decide the following issues such that an order granting Plaintiffs' Motion for Preliminary Injunction may issue:

1. If the Court deems Plaintiffs' request is for a mandatory injunction, whether the law and facts clearly favor Plaintiffs' positions as to their claims for violations of the Electronic Communications Privacy Act, 18 U.S.C. § 2511 (the "ECPA"), violations of the California Invasion of Privacy Act, Cal. Penal Code §§ 631 and 632 ("CIPA"), Intrusion upon Seclusion, and Unfair Competition Law; or alternatively,

2. If the Court deems Plaintiffs' request is for a prohibitory injunction, whether Plaintiffs are sufficiently likely to succeed on the merits of their claims for violations of the ECPA, CIPA, Intrusion upon Seclusion, and Unfair Competition Law;

3. Whether Plaintiffs will likely suffer irreparable harm absent injunctive relief;

4. Whether the balance of equities tips in Plaintiffs' favor; and

5. Whether an injunction is in the public interest.

II. INTRODUCTION

Plaintiffs bring this Motion to stop Google from intercepting and using patient's Health Information (defined further below) from HIPAA and CMIA-covered entities, e.g., Health Care Providers, through its use of the Google Source Code.[3] While the technology might be new, the law is longstanding and clear. Google may not acquire or use patients' Health Information without patients' knowledge and express authorization. Nor may Google acquire the content of a person's communication without authorization, regardless of whether the communication relates to healthcare. Despite these simple rules, Google acquires Health Information through its deployment of the Google Source Code on thousands of Health Care Provider web-properties. It does so in direct violation of federal and state laws – including the ECPA, CIPA, Unfair Competition Law, Cal. Bus. & Prof. Code §§ 17200 *et seq.* ("UCL"), and the common law protection of Intrusion Upon

[3] This Code is associated with Google's advertising systems and products including Google Analytics, Google Ads, Google Display Ads, Google Tag Manager, Google APIs and YouTube.

Seclusion.[4]

There can be no credible dispute of the material facts that show Google's violations. As demonstrated by Google's own documents (cited in the First Amended Complaint; Dkt. No. 16; "FAC") and Plaintiffs' experts, Google designed the Google Source Code to track and re-direct to Google patients' identifiers and the content of patients' communications with their Health Care Providers in real-time. The manner of tracking and interception, as well as the nature of information conveyed, occurs when the Google Source Code is present on a web property and, by design, is common with respect to all patients' who encounter it. *See* Declaration of Plaintiffs' Expert Richard M. Smith ("Smith Decl.") ¶ 67. Upon receipt of patients' Health Information, Google monetizes (i.e., uses the information) within its own advertising systems for purposes of targeted advertising. Importantly, the conduct at issue is not limited to only Plaintiffs' Health Care Providers, but pertains to thousands of web properties and thus likely impacts hundreds of thousands of patients in the U.S. *See* Declaration of Plaintiffs' Expert Timothy Libert ("Libert Decl.") ¶¶ 1-23. Google's tracking and use of patients' Health Information for marketing is all done without patients' knowledge or consent.

Despite being aware of the unlawful conduct underlying these claims, Google has not stopped. Because Google continues to routinely violate the medical privacy rights of Plaintiffs and millions of other Americans, Plaintiffs seek Court intervention to prohibit Google's practices so that patients may enjoy private communications with their Health Care Providers, as is their right. To this end, Plaintiffs seek an Order that will: (1) prohibit Google from intercepting patients' Health Information from Health Care Providers through its use of Google Source Code; (2) prohibit Google from using patients' Health Information that it has intercepted from Health Care Providers through its use of Google Source Code; and (3) separately preserve data relevant to this action. Plaintiffs further request the Court provisionally certify the Class for injunctive relief under Rule 23(b)(2) and

[4] California law applies. Google is headquartered in California, directs its Internet tracking activities from California, and has a binding Terms of Use that adopts California law to govern all disputes with Google Account Holders (in fact, ostensibly with anyone who uses its products and services). It also requires all developers who use its marketing tools to agree to adopt California law to govern all disputes. As such, Google is subject to California law relating to Google Source Code.

appoint Simmons Hanly Conroy LLC ("SHC"), Kiesel Law LLP ("KL"), and Lieff Cabraser Heimann & Bernstein, LLP ("LCHB"), as provisional class counsel under Rule 23(g).

III. STATEMENT OF FACTS

A. The Health Information at Issue Is Protected Under Federal and State Law

As set forth in the FAC, the Health Information at issue includes an individual's status as a patient of a Health Care Provider, unique patient identifiers, the specific actions taken by patients on their Health Care Provider's web properties (e.g., when a patient logs in and logs out of a patient portal, requests an appointment, or seeks information about a specific doctor, condition, treatment, or prescription drug), as well as the content of communications patients exchange with their Health Care Providers. *See* FAC ¶ 2. Content information includes information pertaining to patient registrations, access to, and communications with their Health Care Provider within authenticated webpages (i.e., webpages that require log-in or other authentication, such as a patient portal), as well as information pertaining to patient access to and communications with their Health Care Provider on unauthenticated web pages (e.g., communications relating to specific doctors, appointment requests, symptoms, conditions, treatments, insurance, and prescription drugs). *See id.* ¶¶ 2, 280.

The Health Information at issue constitutes protected health information under federal and California law. *See, e.g.*, HIPAA, 42 U.S.C. § 1320(d-6) and 45 C.F.R. § 160.103; California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.140(v)(1)*;* California Confidentiality of Medical Information Act (CMIA), Cal. Civ. Code § 56.05(i). Further, the information unlawfully obtained by Google more than exceeds the threshold of being capable of identifying an individual under the widely accepted scientific measurement for identifiability – a concept called entropy. *See* Declaration of Plaintiffs' Expert Zubair Shafiq ("Shafiq Decl.") ¶¶ 8-21.

B. The Google Source Code

Google Source Code is designed to track and collect individuals' information when they browse the Internet or use an app. *See* FAC ¶ 32. Google provides the Google Source Code to Health Care Providers in a copy-and-paste format. *Id.* ¶ 33. Once placed on the Health Care Provider's web property, the Google Source Code commands patients' devices to track, intercept, and redirect patients' Health Information to Google. *Id.* ¶ 34. The commandeering of patients' devices occurs through Google Cookies that the Google Source Code deposits on patients' devices. *Id.* ¶ 4. By Google's design, some of these Cookies are disguised as first-party cookies, *i.e.*, the cookies appear to belong to the Health Care Provider with which the patient is directly communicating. *Id.* In truth, the Google Cookies belong to Google, and they allow Google to track and intercept patients' Health Information as the patient navigates through their Health Care Providers' web property. *Id.* As patients exchange communications with their Health Care Providers, the Google Source Code re-directs their Health Information to Google in real-time, *i.e.*, while the patient's communications with their Health Care Providers are still occurring. The redirected Health Information includes communications about doctors, conditions, appointments, and patient portal logins. Plaintiffs describe this process in further detail through the Smith Decl.

C. Case Examples

Health Care Providers typically own and operate a web property that includes a patient portal. *See* Smith Decl. ¶¶ 112 (MedStar), 61 (Kaiser). Both MedStar and Kaiser's web properties have been embedded with the Google Source Code for Google Analytics, as well as other Google products at issue. *Id.* ¶¶ 114 (MedStar), 62, 84 (Kaiser). For example, when a patient first visits the Kaiser web property, the Google Source Code deploys cookies on the patient's computing device. *See id.* ¶¶ 54-60. These cookies include "first-party" cookies that are disguised as belonging to Kaiser and "third-party" cookies from Google associated with its marketing services to advertisers. *Id.* With each communication that a patient exchanges at their Health Care Provider's web property, including the patient portal, the Google Source Code intercepts and transmits to Google Analytics, in real-time: (1) patient identifiers such as IP address, user-agent, and Google Cookies; (2) request URLs; (3) events; and (4) query string parameters. *See* Smith Decl. ¶¶ 67, 114;[5] *see also* FAC ¶ 52.

D. Google Associates the Health Information Collected Across its Systems

After Google receives the information through Google Analytics, Google Ads, Google Display Ads, Google Tag Manager, Google APIs and YouTube, Google publicly states that it connects the identifiers and content in its backend systems for advertisers. *See* FAC ¶¶ 121-23. In

[5] The Smith Decl. describes IP address (¶¶ 167-99), user-agent (¶ 21), request URLs (¶¶ 15, 18, 19), events (¶¶ 68, 86), and query string parameters (¶¶ 13-14).

other words, all of these Google systems and products have interconnected systems for collecting and using the Health Information. Google uses those interconnections to track patients across different devices and different browser-states. For example, Google can track a patient's activity on their desktop, laptop, tablet, and mobile phone and stitch the information together in a single profile.

Likewise, the nature of Google's collection methods enables it to connect a patient's activity while they are signed-in to a Google Account to their activity while not signed into a Google Account. For example, when a patient: (1) signs into their Google Account; (2) leaves the Google pages related to their Google Account; but (3) does not formally sign out of their Google Account, Google will collect the following identifiers for that person on non-Google websites where Google Source Code is deployed: (1) the person's Google Account identifier; (2) a cookie that uniquely identifies their browser-device combination; (3) IP address; (4) user-agent information; and (5) device properties sufficient to uniquely identify the device. If the patient later formally signs-out of their Google Account, Google continues to collect all of the same identifiers except the Google Account identifier. However, because the remaining information uniquely identifies the device – and the previous communication connected those unique identifiers to the Google Account – Google remains readily capable of associating the signed-out data with the signed-in data. In fact, Google advertises that it uses this capability to track conversions – taking credit with advertisers for actions that people take while not signed-in to a Google Account based on Google advertisements they saw while signed in, and vice-versa. *See* FAC ¶ 151. In the context of this case, it means that Google is not only receiving health and personal information that is protected under federal law, but also (for Google Accountholders at least) Google is connecting that same data directly with each patient's Google Account, which includes their name, email address, phone number, and more.

E. <u>The Scope of Google's Misconduct Is Readily Identifiable and Preventable</u>

In a similar action recently brought against Meta concerning its surreptitious tracking on Health Care Provider web properties, the court concluded that facts substantially similar to those set forth here were sufficient to meet many of the elements required for a preliminary injunction. However, the Court explained that it would not grant the motion because of: (1) uncertainty regarding the scope of the defendant's conduct; and (2) the defendant's sworn affidavits that it was trying to fix the problem. *In re Meta Pixel Healthcare Litig. ("Meta Pixel")*, 2022 WL 17869218, at *1 (N.D. Cal. Dec. 22, 2022) (Orrick, J.). Plaintiffs in this action against Google have addressed these issues. *First,* Plaintiffs have identified 6,046 Health Care Provider web properties where Google is collecting Health Information without authorization. *See* Libert Decl. ¶¶ 15-19.[6] *Second*, Plaintiffs submit proof that Google has had specific knowledge of the problem,[7] but its illegal activity has not abated in any way. *See* Libert Decl. ¶ 23. As detailed in the FAC, and set forth in the supporting declaration of Prof. Zubair Shafiq, Google has existing systems – a "crawler" – that can be used to search for and identify Health Care Provider web properties that are subject to HIPAA, e.g., those Health Care Provider web properties that have, in effect, identified themselves to be Health Care Providers by posting the HIPAA Notice of Privacy Practices on its domain.[8] *See* Shafiq Decl. ¶¶ 22-25; *see also* FAC ¶ 241.[9]

Once the crawler identifies the above Health Care Providers, Google can cross-check that list against its own list of properties from which it receives data through Google Analytics, Google Ads, Google Display Ads, Google Tag Manager, Google APIs, and YouTube. As a further cross-check, Google could analyze the communications on identified Health Care Providers' web

[6] Plaintiffs are providing this list to Google with the request that Google admit or deny the HIPAA or CMIA-status of each and the existence of specific Google Source Code at each such property.

[7] Google, *HIPAA and Google Analytics*, available at https://support.google.com/analytics/answer/13297105?hl=en (expressly acknowledging that "HIPAA-regulated entities using Google Analytics must refrain from exposing to Google any data that may be considered Protected Health Information (PHI)").

[8] Federal law requires every Health Care Provider to "prominently post its HIPAA notice on the website and make the notice electronically available through the website." 45 C.F.R. § 164.520(c)(3). It also requires that each HIPAA Notice include the phrase "THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THAT INFORMATION." 45 C.F.R. § 164.520(b)(1)(i). Therefore, the crawler simply need search for that phrase.

[9] The ability to "crawl" web pages on the Internet is not unique to Google. Plaintiffs have also begun this process on behalf of the Class. As explained in the Libert Decl., Dr. Libert was able to identify at least 6,046 Health Care Providers' web properties in the U.S. and determine where the Google Source Code appeared in those web properties. *See* Libert Decl. ¶¶ 16-23. As stated, Plaintiffs will provide Google with this list and request that Google admit or deny which services are present on the properties identified. However, Plaintiffs' ability to do this does not relieve Google of its obligation to identify and ameliorate its own bad conduct. And, Google has an affirmative obligation to engage in this analysis, as identification of the at issue Health Care Providers will be relevant to Google's determination of the scope of its preservation obligations.

properties through Google's "verticals" API. *See* Shafiq Decl. ¶¶ 22-25. As explained by Prof. Shafiq, "verticals" API is a content classification system created by Google that is intended to easily identify the content of a particular web page or app. *See id.* ¶¶ 22-24. In fact, Google publicly admits that its "verticals" API can be used to target at least 89 different health related categories. *See id.* ¶ 22; FAC ¶ 169. Prof. Shafiq opines that Google could, with relative ease, leverage this existing system to search for and identify Health Care Providers. *See id.* ¶ 24. Google could then stop receiving data from the resulting web properties at issue in this action.

IV. LEGAL ARGUMENT

Pursuant to Fed. R. Civ. P. 65, and Civil Local Rules 65-2 and 7-2, Plaintiffs move for a preliminary injunction and seek an order requiring Google to stop its unlawful interception and use of patients' Health Information via Google Source Code.

Injunctive relief is appropriate where a plaintiff establishes: (1) it is likely to succeed on the merits of its claims; (2) it will likely suffer irreparable harm in the absence of injunctive relief; (3) the balance of equities tips in its favor; and (4) an injunction is in the public interest. *Winter v. Natural Res. Def. Council*, 555 U.S. 7, 20 (2008). The most important of the *Winter* factors is "likelihood of success on the merits." *See Disney Enters., Inc. v. VidAngel, Inc.*, 869 F.3d 848, 856 (9th Cir. 2017). To show "likelihood of success on the merits," a plaintiff need not show with absolute certainty that he will prevail. *See Drakes Bay Oyster Co. v. Jewell*, 747 F.3d 1073, 1085 (9th Cir. 2014). Rather, a reasonable probability of success, not an overwhelming likelihood, is all the law requires. *See Gilder v. PGA Tour, Inc.*, 936 F.2d 417, 422 (9th Cir. 1991). Where a plaintiff seeks mandatory injunctive relief (i.e., an order that the responsible party "take action") instead of prohibitory injunctive relief (i.e., an order prohibiting the responsible party from taking action in order to maintain the status quo), such a plaintiff "must establish that the law and facts clearly favor her position, not simply that she is likely to succeed." *Garcia v. Google, Inc.*, 786 F.3d 733, 740 (9th Cir. 2015).

A court must find that a "certain threshold showing" is made on each of the four required elements. *Leiva-Perez v. Holder*, 640 F.3d 962, 966 (9th Cir. 2011). But, under the "sliding scale" approach for preliminary injunctions, "a stronger showing of one element may offset a weaker showing of another." *See Pimentel v. Dreyfus*, 670 F.3d 1096, 1105 (9th Cir. 2012) (*citing All. For The Wild Rockies v. Cottrell*, 632 F.3d 1127, 1131 (9th Cir. 2011)). All four elements are met here.

A. <u>Plaintiffs Seek a Prohibitory Injunction</u>

"A prohibitory injunction prohibits a party from taking action and 'pre-serve[s] the status quo pending a determination of the action on the merits.' . . . A mandatory injunction [on the other hand] 'orders a responsible party to "take action."'" *Marlyn Nutraceuticals, Inc. v. Mucos Pharma GmbH & Co.*, 571 F.3d 873, 878-79 (9th Cir. 2009) (citations omitted); *see FTC v. Neovi, Inc.*, 604 F.3d 1150, 1160 (9th Cir. 2010) (defining prohibitory injunctions as forbidding or restraining an act, and mandatory injunctions as ordering an affirmative act or mandating a specified course of conduct). Here, Plaintiffs request this Court prohibit Google from taking action—intercepting and using patients' Health Information. Plaintiffs anticipate Google will argue that the requested relief, despite its ultimately *prohibitive* effect, amounts to a mandatory injunction because Google may need to verify the scope of its misconduct before turning off the illegal data flow. Notwithstanding, even if this Court finds Plaintiffs seek a mandatory injunction, as explained below, they meet their heightened burden showing the law and facts clearly favor their position, and thus also demonstrate they are likely to succeed on the merits.

B. <u>The Law and Facts Clearly Favor Plaintiffs' Position</u>

This Motion is predicated on Plaintiffs' causes of action for violations of the Wiretap portion of the ECPA and CIPA, the UCL, and for violating common privacy law (i.e., Intrusion upon Seclusion). Regardless of the type of injunction, Plaintiffs demonstrate the law and facts clearly favor their position, satisfying the first *Winter* factor. And, because consent is a common defense for each claim, Plaintiffs address that at the outset.

1. <u>Plaintiffs Did Not Consent to Google's Acquisition or Use of their Health Information</u>

a. <u>HIPAA Required Consent Was Not Obtained</u>

The Health Information at issue, which includes patient status and associated healthcare communications, are protected by federal law. Under HIPAA, a company like Google may not "obtain[] individually identifiable health information relating to an individual" without express authorization. 42 U.S.C. § 1320d-6. Federal law is also clear that patient-status alone is protected information. *See* FAC ¶ 181 n.65. HHS Guidance confirms this: "If [patient identifiers are] listed with health condition, health care provision or payment data, such as an indication that an individual was treated at a certain clinic, then this information would be [protected health information]."[10]

Here, Google's acquisition of Health Information relating to patient portal logins and logouts, activity inside the patient portal, and communications on other pages relating to appointments, services, doctors, conditions, treatments, symptoms, insurance, and more invokes the protections of HIPAA – and its stringent requirements on consent. In *Meta Pixel*, a case with substantially similar facts, the court agreed, holding that the interception of "data relating to patient portal logins and logouts alongside identifiers for each patient" would "reveal[] patient status" and that "patient status is protected health information." 2022 WL 17869218, at *8-9. Google's conduct in this case not only falls along the same lines, but is in fact worse. The *Meta Pixel* case's motion for preliminary injunction did not involve interception of patient communications within the patient portal, whereas here evidence demonstrates that Google intercepts such communications. *See* Smith Decl. ¶¶ 82-94. Google agrees that this violates HIPAA. *See* Google's "HIPAA and Google Analytics" page.[11]

b. <u>General Express and Implied Consent Was Not Obtained</u>

Even in the absence of HIPAA guidelines on consent, it is a defendant's "burden to prove consent." *Calhoun v. Google, LLC,* 526 F. Supp. 3d 605, 620, 623 (N.D. Cal. 2021) (Koh, J.) "Consent 'can be explicit or implied, but any consent must be actual.'" *Id.* at 620. To be actual, "the disclosures must 'explicitly notify' users of the practice at issue" and "must have only one plausible interpretation" – that being in favor of the party claiming consent. *Id.* (*citing Facebook Consumer Privacy User Profile Litig*., 402 F. Supp. 3d 767, 789-94 (N.D. Cal. 2019)).

[10] HHS, *Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule,* https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf at 5 (issued Nov, 26, 2012).

[11] Google, *HIPAA and Google Analytics*, available at https://support.google.com/analytics/answer/13297105?hl=en.

In the Internet context, express consent is often determined by reference to consumer contracts of adhesion. *Silver v. Stripe, Inc.*, 2021 WL 3191752, at *6 (N.D. Cal. Jul. 28, 2021). In doing so, a court must "pretend that users actually read [Google's] contractual language before clicking their acceptance, even though we all know virtually none of them did." *Facebook User Profile*, 402 F. Supp. 3d at 789. The Court must also interpret any purported consent through the eyes of a reasonable person, and where there are multiple plausible interpretations of the contractual language, consent cannot be presumed. *Id.* With respect to implied consent, courts are clear that consent "should not casually be inferred." *In re Pharmatrak, Inc.,* 329 F.3d 9, 20 (1st Cir. 2003). Nor can it "be inferred from the mere purchase of a service, regardless of the circumstances." *Id.* "Without actual notice, consent can only be implied when the surrounding circumstances convincingly show that the party knew about and consented to the interception." *Id.* Critically, "there can be no implied consent in any non-fictitious sense of the term when express consent is procured by a misrepresentation or a misleading omission." *Desnick v. Am. Broad. Companies, Inc.*, 44 F.3d 1345, 1351 (7th Cir. 1995); *see* Restatement (Second) of Torts § 892B(2).

Here, to the extent Google claims that it obtained consent through any contract of adhesion or consumer-facing policy or document, such claim should be rejected. This is because Google makes express promises to the contrary which results in multiple plausible interpretations of those promises. For example, the Google Privacy Policy includes "health information" under the list of "categories of information" that it collects. FAC ¶¶ 219, 226, 449, 452, 476, 494.[12] However, Google limits the statement to "Health information *if you choose to provide it*." *Id.* Elsewhere, Google promises that it "requires that advertisers comply with all applicable laws and regulations in addition to the Google Ads policies." *Id.* ¶¶ 223, 226, 449, 462, 476, 494. The Privacy Policy also incorporates by reference a document that states: "We expect all advertisers to comply with the local laws for any area that their ads target, in addition to the standard Google Ads policies. We generally err on the side of caution in applying this policy because we don't want to allow content of

[12] The statements set forth in the FAC, and sampled herein, apply equally to all Class Members on the issue of consent. This is because Google asserts that these promises apply to anyone who uses its products or services. *See* FAC ¶¶ 212, 492.

questionable legality." *Id.* ¶¶ 223, 224, 226, 449, 464, 476, 494. Google breaches these promises, and others (*see id.* ¶¶ 224, 226, 449, 465) by the conduct described in this Motion. Thus, it cannot claim consent on the basis of any of these documents. *See Desnick*, 44 F.3d at 1351; Restatement (Second) of Torts § 892B(2).

Indeed, there is "no refuge" to a defendant who purports to gain consent through a mistake that defendant knew, or, in the exercise of reasonable care, should have known about that relate to the nature and quality of the invasion intended. *Theofel v. Farey-Jones*, 359 F.3d 1066, 1073 (9th Cir. 2003). That is, consent is not valid where defendant knowingly invites a mistake about "the essential character of the act itself," such as "that which makes it harmful or offensive." *Id.* Determining whether something goes to the "essential nature of the invasion" turns "on the extent to which the intrusion" impacts the specific interests that the claim seeks to protect. *Id.* "Even when no restriction is specified, the reasonable interpretation of consent may limit it to acts at a reasonable time and place, or those reasonable in other respects." Restatement (Second) of Torts § 892A(3), cmt. g. Prosser & Keeton explain: a boxer "consent[s] to the defendant's striking at him" even "if death unexpectedly results" but does not "consent to being hit with brass knuckles, which is the same invasion by an act of different character." W. Page Keeton et al., *Prosser and Keeton on Torts* § 18, 118 (5th ed. 1984); *see also Sanchez-Scott v. Alza Pharms.*, 86 Cal. App. 4th 365, 375 (2001). Plaintiffs have not consented to Google's conduct.

c. <u>There Is No Valid Consent from Health Care Providers</u>

The Health Information that Google intercepts is protected under HIPAA and cannot be disclosed without Plaintiffs' written consent and without the execution of a Business Associate Agreement that ensures confidentiality. *See* 45 C.F.R. § 164.502(e), 164.504(e), 164.508(a). Plaintiffs' Health Care Providers did not obtain Plaintiffs' written consent to divulge, use, or redirect their communications to Google. Likewise, Plaintiffs' Health Care Providers did not enter into a Business Associate Agreement with Google. To this point, Google states it: "makes no representations that Google Analytics satisfies HIPAA requirements and does not offer Business

Associate Agreements in connection with this service."[13] Thus, any purported consent is inadequate because neither Google nor Plaintiffs' Health Care Providers satisfied HIPAA requirements.

2. <u>The Law and Facts Clearly Favor Plaintiffs' ECPA Claim</u>

"The [ECPA] prohibits the unauthorized 'interception' of an 'electronic communication.'" *In re Facebook Internet Tracking Litig.*, 956 F.3d 589, 606 (9th Cir. 2020) (*citing* 18 U.S.C. § 2511(1)(a)-(e)). To prevail, plaintiff must show that Google: (1) intentionally; (2) intercepted; (3) content; (4) related to an electronic communication; (5) by using an electronic, mechanical, or other device." *In re Pharmatrak*, 329 F.3d at 18.

a. <u>Google "Intercepts" Plaintiffs' Health Information</u>

"Intercept" is defined under the ECPA as the "acquisition of the contents of any … electronic … communication through the use of any electronic … or other device." 18 U.S.C. § 2510(f). "Acquisition" means the "act of acquiring, or coming into possession of." *U.S. v. Smith*, 155 F.3d 1051, 1055 n.7 (9th Cir. 1998). "Such acquisition occurs 'when the contents of a … communication are captured or redirected in any way.'" *Noel v. Hall*, 568 F.3d 743, 749 (9th Cir. 2009).

Here, the Google Source Code is designed for the very purpose of intercepting communications on third-party websites by surreptitiously and contemporaneously redirecting those communications to Google. Thus, Google intentionally acquires Plaintiffs' Health Information and communications. The Google Source Code is designed to redirect specific communications (and identifiers) to Google when patients are on their Health Care Providers' web-properties, including the contents of buttons the patient clicked, detailed URLs including information about their doctors, appointments, conditions, and treatments, and other data points that are considered individually identifiable health information as a matter of law under HIPAA, such as IP address, user-agent information, and device properties sufficient to uniquely identify an individual. *See* Smith Decl. ¶¶ 67, 207.

[13] Google, *HIPAA and Google Analytics*, available at https://support.google.com/analytics/answer/13297105?hl=en.

b. Google Acquires the "Content" of Patients' Communications

Google acquires the "contents" of patients' electronic communications, which the ECPA defines as "*any* information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(8) (emphasis added). Here, Google acquires not just "any" information about the substance, purport, or meaning, but, in many cases, the actual communication itself, such as "login" or the name of a button a patient clicks on a Health Care Provider web-property. *See* Smith Decl. ¶¶ 43. Google similarly acquires other such communications. The Smith Declaration details all of the pages on which Google re-directs patient identifiers and content to itself for MedStar Health patients. These include:

- https://www.medstarhealth.org/locations/geriatrics-and-senior-services-washington-hospital-center
- https://www.medstarhealth.org/mymedstar-patient-portal
- https://www.medstarhealth.org/doctors
- https://www.medstarhealth.org/doctors/vandhna-sharma-md

See Smith Decl. ¶ 114.

These types of invasive interceptions are exactly the kind of detailed information that courts have routinely found to be "content" under the Wiretap Act. For example, in *Meta Pixel* the Court explained that "log-in buttons and the kind of descriptive URLs identified in the Smith Decl. are 'contents' within the meaning of the statute." 2022 WL 17869218, at *11. In doing so, the court specifically cited to the following examples of "content":

- hartfordhospital.org/services/digestive-health/conditions-we-treat/colorectal-small-bowel-disorders/ulcerative-colitis;
- wwwmedstarhealth.org/sxa/search/results/q=diabetes; and
- https://www.medstarhealth.org/doctors/paul-a-sack-md.

Id. at *11; *see also Facebook Internet Tracking*, 956 F.3d at 605; *In re Pharmatrak*, 329 F.3d at 18; *In re Google RTB Consumer Priv. Litig.*, 2022 WL 2165489, at *10 (N.D. Cal. Jun. 13, 2022); *In re Google, Inc. Cookie Placement Consumer Privacy Litig.*, 806 F.3d 125, 137 (3d Cir. 2015).

c. Plaintiffs' Claims Involved "Electronic Communications"

Likewise, Google cannot dispute that "electronic communications" are at issue here. The

ECPA defines an "electronic communication" as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects interstate … commerce[.]" 18 U.S.C. § 2510(12).[14] Patient communications with their Health Care Providers on provider web-properties fit within this broad definition.

d. Google's Actions Occur through "Devices"

Next, Google's actions occur through several "devices" within the meaning of 18 U.S.C. § 2510(5). These include cookies, the patient's browsers, the patient's computing devices, Google's web-servers, the web-servers of the healthcare provider properties, and the Google Source code deployed by Google to effectuate its acquisition of patient communications. Each of these constitute "devices" under the Wiretap Act. *See U.S. v. Szymuszkiewicz*, 622 F.3d 701, 707 (7th Cir. 2010); *In re Carrier IQ, Inc. Cons. Privacy Litig*., 78 F. Supp. 3d 1051, 1084-87 (N.D. Cal. 2015).

e. Google's Actions Are Without Authorization

Google's interception of the contents of Plaintiffs' electronic communications was and is without Plaintiffs' authorization. As set forth above, Google did not obtain valid consent or authorization from Plaintiffs and Class Members, and Google did not obtain valid consent from the Health Care Providers.

Further, while the ECPA contains an exception to liability where a "party" to the communication has consented (18 U.S.C. § 2511(2)(d)), this exception does not apply where a "communication is intercepted for the purpose of committing any criminal or tortious act." 18 U.S.C. § 2511(2)(d). Thus, any claim by Google that it obtained purported consent from a Health Care Provider would not absolve it of liability under the ECPA. Google acquired Plaintiffs' and Class Members' private Health Information with the requisite intent to violate 42 U.S.C. § 1320d-6; state unfair business practices statutes; Art. I, section 1 of the California Constitution; common law trespass upon Plaintiffs' personal and private property; and the California Comprehensive Data Access and Fraud Act. Any of these is sufficient to fall within the "committing any criminal or

[14] While there are exceptions to this definition, none apply in this case.

tortious act" provision of Section 2511(2)(d). Google therefore cannot avail itself of a consent defense under the ECPA. As explained in *Sussman v. ABC*, the focus of Section 2511(2)(d) is "whether the purpose for the interception – its intended use – was criminal or tortious." 186 F.3d 1200, 1202 (9th Cir. 1999). "Where the taping is legal, but is done for the purpose of facilitating some further impropriety … section 2511 applies." *Id.* The Court further explained: "the existence of [a] lawful purpose would not sanitize a tape that was also made for an illegitimate purpose." *Id.*; *see Deteresa v. ABC*, 121 F.3d 460, 467 n.4 (9th Cir. 1997) (Section 2511 applies where defendant taped the conversation for purpose of violating Cal. Penal Code § 632, invading her privacy, defrauding her, or committing unfair business practices, and noting lower courts held that trespass, violation of state computer crime laws, breach of fiduciary duty, and planned subsequent use for a tortious purpose also satisfy 2511). The provisions of Section 2511 clearly apply here. Suppose Google had carried out its scheme without the use of Internet technologies. Instead of source code, Google obtained a hard-copy database with summaries of patient communications with their Health Care Providers – and then used that information to create profiles about individuals, to, in turn, send direct mail or other marketing materials. There is no doubt that this conduct would be tortious and criminal. As such, it satisfies the *Sussman* test.[15]

Courts have also consistently held that the conduct at issue here gives rise to claims for tortious and statutory liability. *See Doe v. Virginia Mason*, 2020 WL 1983046, at *2 (Wash. Super. Feb. 12, 2020); *see also* Barnes Decl., Ex. A (*Doe v. MedStar*, Case No. 24-C-20-000591 (Baltimore City, Maryland) (actionable for violation of state Wiretap Act, Intrusion Upon Seclusion, and other claims), Ex. D (*Doe v. Partners*, Case No. 1984-cv-01651 (Suffolk Cty, Mass.) (actionable violation of state Wiretap Act, Intrusion Upon Seclusion and other claims); *see also* Barnes Decl., Ex. B (*Doe v. Mercy Health*, Case No. A2002633 (Hamilton County, Ohio), Ex. C (*Doe v. University Hospitals*, Case No. CV-209333357 (Cuyahoga County, Ohio), Ex. E (*Doe v. Sutter Health*, Case No. 34-

[15] To the extent that Google argues that a business "acting for commercial gain" cannot have a criminal or tortious purpose, this is incorrect. Lawful business activity would never have a criminal purpose and rarely (perhaps never) a tortious purpose. However, Google's activity here is not lawful. Put simply, not all "commercial activity" is protected. For example, the recording in *U.S. v. Lam*, 271 F. Supp. 2d 1182, 1184 (N.D. Cal. 2003), was made for a commercial purpose – to make money from illegal gambling. But that did not remove the recording from 2511(2)(d).

2019-00258072-CU-BT-GDS (Sacramento County, California).[16]

For the reasons set forth above, the law and facts clearly favor Plaintiffs' ECPA claim.

3. <u>The Law and Facts Clearly Favor Plaintiffs' CIPA Claim</u>

CIPA mirrors the federal Wiretap Act with a few important differences. First, California is an all-party consent state. For the reasons stated above, Google has failed to obtain consent from all parties. Second, CIPA does not require the defendant to use a device. Instead, it prohibits interception "by means of any machine, instrument, or contrivance, or in any other manner[.]" Cal. Penal Code § 631(a). Third, CIPA creates liability for anyone – including parties to the communication – who records a "confidential communication" without authorization by means of "any electronic amplifying or recording device." Cal. Penal Code § 632.

Plaintiffs' communication with their Health Care Providers was "confidential" because it was "carried on in circumstances" that would reasonably indicate that the parties "desired it to be confined to the parties thereto." Cal. Penal Code § 632(c). In fact, Plaintiffs' communications with their Health Care Providers are confidential as a matter of law under HIPAA, the CMIA, and Cal. Penal Code § 632.01, providing enhanced penalties for disclosure or distribution (in any manner), "the contents of a confidential communication with a health care provider." In *Meta Pixel*, on a motion for preliminary injunction, the court found that plaintiffs in that case would likely be able to show the communications there were confidential under CIPA under substantially similar facts to those alleged here. 2022 WL 17869218, at *15. Based on the foregoing, the law and facts clearly favor Plaintiffs' CIPA claim.

4. <u>The Law and Facts Clearly Favor Plaintiffs' Intrusion Upon Seclusion Claim</u>

Intrusion upon seclusion requires a showing that: (1) a defendant intentionally intruded into a place, conversation, or matter as to which the plaintiff has a reasonable expectation of privacy; and (2) … the intrusion was 'highly offensive' to a reasonable person." *In re Google RTB Consumer Priv. Litig.*, 2022 WL 2165489, at *7. Although "[c]ourts are generally hesitant to decide claims of

[16] Counsel for Plaintiffs here represented the patient-plaintiff classes in each of the cited cases.

this nature at the pleading stage," the *Meta Pixel* court found that substantially similar claims against Meta were "fairly strong." 2022 WL 17869218, at *15.

The first element is satisfied where a company "set[s] an expectation" that certain "data would not be collected, but then collected it anyway." *Facebook Internet Tracking*, 956 F.3d at 602. Plaintiffs satisfy that element here. Google's Privacy Policy states that it may collect "health information," but immediately qualifies that disclosure with "if you choose to provide it." But as discussed above, Plaintiffs never chose to provide this data.

In addition to a company's promises, a court must consider the nature of the information at issue. Here, "health-related communications with a medical provider are almost uniquely personal." *Meta Pixel*, 2022 WL 17869218, at *14. "One can think of few subject areas more personal and more likely to implicate privacy interests than that of one's health or genetic make-up." *Norman-Bloodsaw v. Lawrence Berkeley Lab.*, 135 F.3d 1260, 1269 (9th Cir. 1998); *Facebook User Profile*, 402 F. Supp. 3d at 783. In *Meta Pixel*, the Court found that "plaintiffs will likely be able to show that they had an objectively reasonable expectation that their communications with their medical providers were confidential." 2022 WL 17869218, at *14.

Finally, a legal prohibition on access to information unless certain conditions are met can create a reasonable expectation of privacy. Here, the information at issue is protected by federal and state law against unauthorized acquisition. *See* 42 U.S.C. § 1320d-6. This alone is sufficient.

To determine the second element, courts may consider "the degree of the intrusion, the context, conduct and circumstances surrounding the intrusion as well as the intruder's motives and objectives, the setting into which he intrudes, and the expectation of those whose privacy is invaded." *Hill v. NCAA*, 7 Cal. 4th 1, 26 (1994). In *Meta Pixel*, the Court found:

> There is support for plaintiffs' position that Meta has behaved egregiously. By enacting criminal and civil statutes forbidding the disclosure of protected health information without proper authorization, Congress has made policy decisions regarding the importance of safekeeping this information. *See, e.g.* 42 U.S.C. § 1320d-6 … 45 CFR § 164.508. … Courts have also found that taking personal contact information without consent could be deemed highly offensive. *See Opperman v. Path*, 87 F. Supp. 3d 1018, 1060-61 (N.D. Cal. 2014).
>
> It is true that '[c]ourts in this district have consistently refused to characterize the disclosure of common, basic digital information to third parties as serious or egregious violations of social norms.' *In re Google Inc. Privacy Policy*, 58 F. Supp.

> 3d 968, 985 (N.D. Cal. 2014). But that is not the kind of information here. Meta does not point to a single case where a court found that the collection of the kinds of information at issue here did not constitute a highly offensive invasion of privacy.

2022 WL 17869218, at *16. Therefore, the law and facts clearly favor Plaintiffs' Intrusion claim.

5. **The Law and Facts Clearly Favor Plaintiffs' UCL Claim**

The unlawful conduct complained of herein violates the UCL. "The 'unlawful' practices prohibited by section 17200 are any practices forbidden by law, be it civil or criminal, federal, state, or municipal, statutory, regulatory, or court-made." *Saunders v. Superior Court*, 27 Cal. App. 4th 832, 838-39 (1994). As explained above, Google's conduct violates the ECPA, CIPA, common law and also HIPAA (which although not independently actionable, can be a basis for a UCL unlawful claim, *see Rose v. Bank of Am., N.A.*, 57 Cal. 4th 390, 396-97 (2013)). Plaintiffs and Class Members relied on Google's representation that it will not collect Health Information without user's consent was untrue. *See* FAC ¶ 361. And, had Plaintiffs and Class Members known the truth of Google's conduct, they would not have used the Health Care Provider websites. *See id.* ¶ 362; *see also Daniel v. Ford Motor Co.*, 806 F.3d 1217, 1225 (9th Cir. 2015) (explaining omissions case proven by showing "that, had the omitted information been disclosed, one would have been aware of it and behaved differently[]'"). Finally, there is no question that a loss of money or property has occurred as demonstrated by the fact that Google is able to use and sell the information within its various advertising systems. While only an identifiable "trifle" of injury is needed to be shown (*Kwikset Corp. v. Superior Court*, 51 Cal. 4th 310, 321-24 (2011)), Plaintiffs value their Health Information far more than that. And Google's disclosure of this confidential and valuable information has now diminished the value of such information. *See* FAC ¶¶ 358, 488, 507.

C. **Plaintiffs Are Irreparably Harmed By Google's Conduct**

A plaintiff must show that "irreparable injury is likely in the absence of an injunction." *Winter*, 555 U.S. at 22. That is, the harm must be one "for which there is no adequate legal remedy, such as damages." *Arizona Dream Act Coal v. Brewer*, 757 F.3d 1053, 1068 (9th Cir. 2014) (citation omitted); *Marlyn Nutraceuticals, Inc.*, 571 F.3d at 879 (mandatory injunction granted if very serious damage will result or if injury complained of not compensable in damages). The harm alleged here falls squarely within this standard. *See Meta Pixel*, 2022 WL 17869218, at *17 (on similar facts, "[t]he invasion of privacy triggered by the [Meta] Pixels' allegedly ongoing disclosure of plaintiffs' medical information is precisely the kind of intangible injury that cannot be remedied by damages").

Further, as the Ninth Circuit observed: "A dangerous act, if committed often enough, will inevitably lead to harm, which could easily be irreparable." *Inst. of Cetacean Research v. Sea Shepherd Conservation Soc'y*, 725 F.3d 940, 946 (9th Cir. 2013). That is precisely the situation here. Plaintiffs' evidence shows that Google continues to unlawfully track, collect and monetize Plaintiffs' and Class members' Health Information. In fact, in an analysis of 6,046 Health Care Provider web properties, Google Source Code was found on **87%** of them. *See* Libert Decl., ¶ 23. Given this percentage, it is clear that Google's conduct is pervasive and ongoing such that the probability of harm attributable to Google is not just "likely" but ***virtually certain*** to occur absent the requested injunctive relief.

Additionally, while it is true that the Class can economically measure their damages, it is also true that the underlying privacy violations cannot be remedied by money damages. This is not a trade secret or copyright infringement case where the party seeking to enforce their singular right over the information at issue does so in order to protect its inherent economic value. No medical patient seeks to maintain their medical privacy for the purposes of preserving its financial value. Rather, they zealously guard the secrecy of such information for the purposes of the secrecy itself. Once that right to privacy has been violated, it can be compensated but never remedied. For this reason, the Ninth Circuit has recognized that "intangible injuries" qualify as irreparable harm. *Arizona Dream Act Coal.*, 757 F.3d at 1068 ("No award of damages can compensate Plaintiffs' for the myriad personal and professional harms caused by their inability to obtain driver's licenses."); *Enyart v. Nat'l Conference of Bar Examiners, Inc.*, 2010 WL 475361, at *7 (N.D. Cal. Feb. 4, 2010), *aff'd*, 630 F.3d 1153 (9th Cir. 2011) (finding risk of "a serious career setback" for plaintiff and resulting psychological impact sufficient to establish irreparable harm); *Doe 1 v. U.S. Dep't of Homeland Sec.*, 2020 WL 6826200, at *8 (C.D. Cal. Nov. 20, 2020), *aff'd sub nom. Does 1 through 16 v. U.S. Dep't of Homeland Sec.*, 843 F. App'x 849 (9th Cir. 2021) (holding "each of these Plaintiffs is, or will imminently be, harmed by the inability to train and practice with their teams—a critical activity in furthering their athletic careers.").

Because Plaintiffs and Class members suffered and continue to suffer imminent and irreparable harm by Google's actions, injunctive relief is appropriate. As just one example, Plaintiffs want to continue to communicate with their Health Care Providers through online platforms but have no practical way of knowing if their communications are being intercepted by Google, and thus continue to be at risk of harm from Google's conduct. *See* FAC ¶ 310, 323.

D. <u>The Balance of Equities Tips Sharply in Plaintiffs' Favor</u>

A plaintiff seeking injunctive relief must establish that the balance of equities tips in its favor. *See Winter*, 555 U.S. at 20. In balancing the equities, courts look to "the competing claims of injury and must consider the effect on each party of the granting or withholding of the requested relief." *Id.* at 24. When courts are faced with "a conflict between financial concerns and preventable human suffering," they have "little difficulty concluding that the balance of hardships tips decidedly in plaintiffs' favor." *Harris v. Bd. of Supervisors*, 366 F.3d 754, 766 (9th Cir. 2004) (*quoting Lopez v. Heckler*, 713 F.2d 1432, 1437 (9th Cir. 1983)).

An injunction preventing Google from intercepting and utilizing patient Health Information merely requires compliance with HIPAA, the Wiretap Act, CIPA, and other state laws. *See, e.g.*, *Pyro Spectaculars North, Inc. v. Sousa*, 861 F.Supp. 2d 1079, 1092 (E.D. Cal. 2012) (holding injunction would not cause significant hardship to defendant because "it would essentially only require him to abide by existing law."). On the other hand, if Google continues to unlawfully acquire and utilize Plaintiffs' personal and medical information and communications without consent, Plaintiffs and the Class will continue to face serious and substantial irreparable harm. Each day that goes by, more and more individuals unknowingly fall victim to Google's scheme, and the Class is thereby enlarged. *See Indep. Living Ctr. of S. Cal., Inc. v. Shewry*, 543 F.3d 1047, 1049 (9th Cir. 2008) ("When the balance of harm 'tips decidedly toward the plaintiff,' injunctive relief may be granted . . . ."). Moreover, Plaintiffs submit proof that Google has had specific knowledge of the problem,[17] but its illegal activity has not abated in any way. *See* Libert Decl. ¶ 23 (confirming that,

[17] *See* Google's "HIPAA and Google Analytics" page, https://support.google.com/analytics/answer/13297105?hl=en.

out of 6,046 Health Care Provider web properties scanned, Google Source Code continues to be on 87% of them). Thus, any preventative measures that Google claims are in place are not credible. Because the balance of equities tips sharply in Plaintiffs' favor, injunctive relief is appropriate.

E. **The Injunctive Relief Sought Is in the Public Interest**

The public interest weighs heavily towards granting Plaintiffs the relief they seek. Widespread recognition of privacy as a fundamental right precedes this nation's founding. *See Griswold v. Connecticut*, 381 U.S. 479, 486 (1965) ("We deal with a right of privacy older than the Bill of Rights"); *Berger v. New York*, 388 U.S. 41, 45 (1967) (*citing* 4 Blackstone, Commentaries 168 (1765), describing "eaves-droppers" as "a common nuisance . . . preventable at the court, or . . . indictable at the sessions."). The value of this right to individuals is paramount. *See Kewanee Oil v. Bicron*, 416 U.S. 470, 487 (1974) ("A most fundamental human right, that of privacy, is threatened when industrial espionage is condoned or is made profitable; the state interest in denying profit to such illegal ventures is unchallengeable.").

As the Ninth Circuit has pointed out, "One can think of few subject areas more personal and more likely to implicate privacy interests than that of one's health[.]" *Norman-Bloodsaw v. Lawrence Berkeley Lab.*, 135 F.3d at 1269. In *Riley v. California*, a unanimous Supreme Court held that Americans have a reasonable expectation of privacy in the type of data at issue in this case. 573 U.S. 373, 395-96 (2014) ("[C]ertain types of data are also qualitatively different. An Internet search and browsing history … could reveal an individual's private interests or concerns – perhaps a search for certain symptoms of disease, coupled with frequent visits to WebMD."). American courts have long protected this right to privacy. The late Prof. Edward Bloustein explained why:

> The fundamental fact is that our Western culture defines individuality as including the right to be free from certain types of intrusions. This measure of personal isolation and personal control over the conditions of its abandonment is of the very essence of personal freedom and dignity, is part of what our culture means by those concepts. A man whose home may be entered at the will of another, whose conversation may be overheard at the will of another, whose marital and family intimacies may be overseen at the will of another, is less of a man, has less human dignity, on that account. He who may intrude upon another at will is the master of the other and, in fact, intrusion is a primary weapon of the tyrant.

Edward J. Bloustein, *Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser*, 39 N.Y.U. L. Rev. 962, 973-74 (1964).

As discussed above, the public's overarching interest in privacy, particularly as to matters concerning healthcare data, and even more specifically patient-healthcare provider communications, patient status, and patient portal use information, is evidenced by the statutory protections that exist for such sensitive information, including HIPAA, the Wiretap Act, and CIPA. Unless this Court issues an injunction, Google will continue to ignore its duties under the Wiretap Act, CIPA, and other state laws restricting disclosure of confidential information. Therefore, because the injunction sought is in the public interest, injunctive relief is appropriate.

F. <u>No Bond Should Be Imposed</u>

Rule 65(c) gives courts "discretion as to the amount of security required, if any." *Jorgensen v. Cassiday*, 320 F.3d 906, 919 (9th Cir. 2003). Dispensing with a bond is appropriate when "requiring security would effectively deny access to judicial review," particularly when the likelihood of success on the merits favors little or no bond. *California ex rel. Van de Kamp v. Tahoe Reg'l Planning Agency*, 766 F.2d 1319, 1325, *as modified by* 775 F.2d 998 (9th Cir. 1985). Here, Plaintiffs are ordinary healthcare patients who should not be required to post security. The law and facts clearly favor their position, and granting injunctive relief is in the public interest. The Court should thus exercise its discretion to dispense with requiring a bond.

V. <u>THE COURT SHOULD PROVISIONALLY CERTIFY THE CLASS</u>

"Courts in the Ninth Circuit 'routinely grant provisional class certification for purposes of entering injunctive relief.'" *Ahlman v. Barnes*, 445 F. Supp. 3d 671, 682 (C.D. Cal. 2020); *accord Roman v. Wolf*, 977 F.3d 935, 944-45 (9th Cir. 2020); *Meyer for Portfolio Recovery Assoc., LLC*, 707 F.3d 1036, 1041-43 (9th Cir. 2012). Here for purposes of entering a preliminary injunction, the Court should provisionally certify the following class: "All persons in the United States whose Health Information was obtained by Google from their Health Care Provider."

A. <u>The Requirements of Rule 23(A) Are Satisfied</u>

<u>Numerosity</u>: The class is sufficiently numerous under Rule 23(a)(1). Plaintiffs' analysis reveals that, a review of 6,046 Health Care Providers shows that the Google Source Code appears 87% of the time. *See* FAC ¶ 120; Libert Decl. ¶ 23. Given these numbers, logic dictates that even at its most conservative estimate the class of individuals whose Health Information was unlawfully

acquired by Google far exceeds the threshold 40 members. *See Rannis v. Recchia*, 380 F. App'x 646, 651 (9th Cir. 2010) (numerosity satisfied "when a class includes at least 40 members").

Commonality: Commonality under Rule 23(a)(2) is satisfied. "A common question is one where 'the same evidence will suffice for each member to make a prima facie showing [or] the issue is susceptible to generalized, class-wide proof.'" *Tyson Foods, Inc. v. Bouaphakeo*, 577 U.S. 442, 453 (2016). "[T]he threshold for meeting the commonality requirement is relatively low." *Senne v. Kansas City Royals Baseball Corp.*, No. 14-cv-00608-JCS, 2021 WL 3129460, at *18 (N.D. Cal. July 23, 2021). "[A]ll that Rule 23(a)(2) requires is a single significant question of law or fact." *Abdullah v. U.S. Sec. Assocs., Inc.*, 731 F.3d 952, 957 (9th Cir. 2013); *see also Meyer*, 707 F.3d at 1041 ("The existence of shared legal issues with divergent factual predicates is sufficient, as is a common core of salient facts coupled with disparate legal remedies within the class."). Here, all Class Members are subject to Google's practice of tracking and collecting Health Information from their Health Care Providers. The Class's claims under CIPA and the ECPA present numerous common issues of law and fact, including whether Google intercepts patients' "communications" while they are "in transit" or "passing over any wire" within the meaning of theses statutes, and how the Google Source Code effectuates the interception of patient communications. *See also* FAC ¶ 314 (setting forth additional common questions). Each of these questions is central to resolving Plaintiffs' CIPA and ECPA claims and is susceptible of class-wide proof. *See, e.g.*, Smith Decl. (evidencing how the Google Source Code operates). Thus, each of these questions suffices as a "common" issue under Rule 23(a)(2). *See Ruiz Torres v. Mercer Canyons Inc.*, 835 F.3d 1125, 1133 (9th Cir. 2016) (the common question inquiry turns on the "capacity of a classwide proceeding to generate common answers apt to drive the resolution of the litigation.") (internal quotations omitted); *Yahoo*, 308 F.R.D. at 590-91 (commonality satisfied for CIPA claim based on common issues of whether Yahoo intercepted emails while they were passing over a wire or being sent or received within California).

Typicality: Rule 23(a)(3)'s typicality requirement is satisfied. "[T]ypicality refers to the nature of the claim or defense [of the class representative]…and not to the specific facts from which it arose or the relief sought." *Ruiz Torres*, 835 F.3d at 1141. "The test of typicality is whether other members have the same or similar injury, whether the action is based on conduct which is not unique to the named plaintiffs, and whether other class members have been injured by the same course of conduct." *Id.* (*quoting Hanon v. Dataproducts Corp.*, 976 F.2d 497, 508 (9th Cir. 1992)); *see Parsons v. Ryan*, 754 F.3d 657, 685 (9th Cir. 2014) ("Under the rule's permissive standards, representative claims are 'typical' if they are reasonably coextensive with those of absent class members; they need not be substantially identical[]"). Here, Plaintiffs' claims arise from the same challenged practices and rely on the same legal arguments as other Class Members' claims. Like all Class Members, Google intercepted Plaintiffs' Health Information without authorization, and they have suffered and continue to suffer irreparable harm as a result of Google's misconduct (which is ongoing). *See* Barnes Decl., Ex. F (John Doe I), Ex. G (John Doe II), Ex. H (Jane Doe I), Ex. I (Jane Doe II), Ex. J (Jane Doe III), Ex. K (Jane Doe IV), Ex. L (Jane Doe V).

Adequacy: Rule 23(a)(4)'s adequacy requirement is satisfied. Plaintiffs and their counsel have no conflicts of interest with other Class Members and will vigorously prosecute the action. *See Ellis v. Costco Wholesale Corp.*, 657 F.3d 970, 985 (9th Cir. 2011).

B. Under Rule 23(B)(2), the Challenged Conduct Applies Generally to the Class

In addition to the Rule 23(a) requirements, Plaintiffs must satisfy Rule 23(b)(2), which provides that injunctive classes can be certified where Google "has acted or refused to act on grounds that apply generally to the class," making preliminary injunctive relief appropriate under Rule 23(b)(2). Fed. R. Civ. P. 23(b)(2); *Amchem Prod., Inc. v. Windsor*, 521 U.S. 591, 614 (1997). Rule 23(b)(2) "[o]rdinarily will be satisfied when plaintiffs have described the general contours of an injunction that would provide relief to the whole class, that is more specific than a bare injunction to follow the law, and that can be given greater substance and specificity at an appropriate stage in the litigation through fact-finding, negotiations, and expert testimony." *Parsons*, 754 F.3d at 689 n.35 (9th Cir. 2014). "That inquiry does not require an examination of the viability or bases of the class members' claims for relief." *Id.* at 688 (*citing Rodriguez v. Hayes*, 591 F.3d 1105, 1125 (9th Cir. 2010)). Rather, the relevant question is "whether class members seek uniform relief from a practice applicable to all of them." *Rodriguez*, 591 F.3d at 1125. "The fact that some class members may have suffered no injury or different injuries from the challenged practice does not prevent the class from meeting the requirements of Rule 23(b)(2).” *Id*.

The requirements of Rule 23(b)(2) are satisfied here. As laid out above, the injunctive relief sought will provide relief to all Class Members and is specific in the relief sought. Plaintiffs and the Class are subject to the same interception process via the Google Source Code when communicating on their Health Care Providers’ web-properties. The specific relief sought is tailored to address Google Source Code on Health Care Providers’ web-properties and would provide relief to each member of the Class without individualized inquiries. *See Adkins v. Facebook, Inc.*, 424 F. Supp. 3d 686, 698 (N.D. Cal. 2019) (certifying injunctive relief class where plaintiffs sought to compel Facebook to fix data security flaws identified by third-party auditors); *In re Yahoo Mail Litig.*, 308 F.R.D. 577, 601 (N.D. Cal. 2015) (certifying injunctive relief California-only subclass under CIPA and nationwide injunctive relief class under ECPA for Yahoo’s privacy violations in scanning and analyzing consumer emails); *Romero v. Securus Techs., Inc.*, 331 F.R.D. 391, 413 (S.D. Cal. 2018) (certifying injunctive relief class for CIPA violations related to eavesdropping on telephone calls).

C. <u>Plaintiffs’ Counsel Should Be Appointed Provisional Class Counsel</u>

The Court should appoint Plaintiffs’ counsel SHC, KL, and LCHB as provisional class counsel under Rule 23(g). The firms have performed substantial work identifying and investigating potential claims, have significant experience prosecuting class actions and other complex cases with claims similar to those at issue here, are knowledgeable regarding the applicable law, and have the resources and ability to litigate this case. *See* Fed. R. Civ. P. 23(g)(1); Barnes Decl., Ex. M (Simmons Hanly Conroy Firm Bio), Ex. N (Kiesel Law Firm Bio), Ex. O (Lieff Cabaser Heimann & Bernstein, LLP Firm Bio).

VI. <u>CONCLUSION</u>

For the foregoing reasons, Plaintiffs request the Court provisionally certify the proposed class under Rule 23(b)(2), appoint interim class counsel, and enter a preliminary injunction as set forth in the Notice of Motion and accompanying Proposed Order.

DATED: June 13, 2023

KIESEL LAW LLP

By: *<u>/s/ Jeffrey A. Koncius</u>*

Paul R. Kiesel
Jeffrey A. Koncius
Nicole Ramirez

SIMMONS HANLY CONROY LLC
Jason 'Jay' Barnes (admitted *pro hac vice*)
An Truong (admitted *pro hac vice*)
Eric Johnson (admitted *pro hac vice*)

LIEFF CABRASER HEIMANN & BERNSTEIN, LLP
Michael W. Sobol
Douglas Cuthbertson
Melissa Gardner

Attorneys for Plaintiffs and the Proposed Class